219.40074X00
LID#: 18107/P11701

UNITED STATES PATENT APPLICATION

FOR

BLUETOOTH™ BASED SECURITY SYSTEM

INVENTOR:

Sundeep M. Bajikar

Express Mail Label No. EV 339 909 705 US

Prepared By:

Antonelli, Terry, Stout & Kraus, LLP
Suite 1800
1300 North Seventeenth Street
Arlington, Virginia 22209
Tel: 703/312-6600
Fax: 703/312-6666

BLUETOOTH™ BASED SECURITY SYSTEM

Technical Field

The present invention relates to a security system, and more particularly, relates to an ad-hoc security system for electronic devices such as portable computers equipped with Bluetooth™ for providing access control, tracking and security services of varying complexity without any additional hardware overheads.

Background

Electronics devices such as notebook and laptop computers have become increasingly compact and portable and, as a result, increasingly vulnerable to unauthorized use, theft or loss. This is because these portable computers are small, expensive and may contain very valuable information.

Many computers, especially portable computers, have been secured from unauthorized use, theft or loss by mechanisms based on principles of prevention, deterrence or recovery. Prevention mechanisms may include physical locking devices which lock portable computers to docking stations. Deterrence mechanisms may include myriad alarm systems which employ various deterrence methods, including sound and visual alarms to deter an unauthorized person or a thief from stealing the portable computers. Recovery mechanisms may include various systems for providing automatic disabling of portable computers and/or for locating and tracking

stolen portable computers for recovery via existing radio communication infrastructures or existing cellular network infrastructures.

One typical example of computer tracking systems for locating stolen computers is the use of a software (location tracking program) installed to instruct the computer to call a third party monitoring service at regular intervals. When the computer calls the monitoring service, the computer establishes a data link and transmits data to the monitoring service that identifies the computer. When the monitoring service receives a call from the user's computer, the monitoring service is able to determine the location of the computer by utilizing Caller ID. The location of the computer may then be forwarded to a law enforcement agency so that the lost or stolen computer can be retrieved by the law enforcement agency.

Alternatively, the location tracking program may also be installed to identify if an e-mail is being sent from the lost or stolen computer and compare a sender address to a predetermined owner address. If the sender address matches the owner address, the e-mail is sent unimpeded. However, if the sender address does not match with the sender address, then the e-mail is re-directed to a third party such as a law enforcement agency to notify that the computer may have been stolen. However, such location tracking systems are not optimal because a third party monitoring service is required.

Another example location tracking systems are known as Radio Frequency Identification (RFID) systems which are available to uniquely identify and track devices equipped with RFID tags as disclosed, for example, in U.S. Patent No. 6,232,870 for *Applications For Radio Frequency Identification Systems* issued to Garber et al., U.S. Patent No. 6,100,804 for *Radio*

Frequency Identification System issued to Brady et al., U.S. Patent No. 5,963,134 *for Inventory System Using Articles With RFID Tags* issued to Bowers et al., and U.S. Patent No. 5,838,253 for *Radio Frequency Identification Label* issued to Wurz et al. A typical RFID tag (also known as transponder) consists of a semiconductor chip having RF circuits, control logic, memory and an antenna (and a battery in the case of active tags) mounted to a substrate for providing remote identification. However, such RFID systems require dedicated wireless communications, and contain no general wireless data communications capabilities. Another drawback is that the user has purchase the RFID tags, the tag reader, and setup the environment specifically for the RFID service. RFID tags can also be cost prohibitive as each RFID tag can vary from 50 cents to $150 based on the desired capabilities.

Accordingly, there is a need for a new type of asset security and wireless tracking system for electronic devices such as portable computers that can be easily and effectively implemented with an industry standard communications wireless technology such as Bluetooth™ to provide access control, tracking and security services of varying complexity without any additional hardware overheads.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of exemplary embodiments of the present invention, and many of the attendant advantages of the present invention, will become readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols

indicate the same or similar components, wherein:

FIG. 1 illustrates an example Bluetooth™ based security system according to an embodiment of the present invention;

FIG. 2 illustrates an example system platform of a security server (SS) according an embodiment of the present invention;

FIG. 3 illustrates an example system platform of a secured device (SD) such as a portable computer according an embodiment of the present invention;

FIG. 4 illustrates an example Bluetooth transceiver of the secured device (SD) according to an embodiment of the present invention;

FIG. 5 illustrates an example GPS receiver (sensor) of the secured device (SD) according to an embodiment of the present invention;

FIG. 6 illustrates an example Bluetooth and GPS subsystem of the secured device (SD) according to an embodiment of the present invention;

FIG. 7 illustrates an example lock activation procedure between a security server (SS) and a secured device (SD) of the Bluetooth™ based security system according to an embodiment of the present invention;

FIG. 8 illustrates an example parameter exchange procedure for locking between a security server (SS) and a secured device (SD) of the Bluetooth™ based security system according to an embodiment of the present invention;

FIG. 9 illustrates an example lock maintenance procedure of the Bluetooth™ based security system according to an embodiment of the present invention;

FIG. 10 illustrates an example search and arrest procedure of the Bluetooth™ based security system according to an embodiment of the present invention; and

FIG. 11 illustrates an example lock deactivation procedure of the Bluetooth™ based security system according to an embodiment of the present invention.

DETAILED DESCRIPTION

The present invention is applicable for use with all types of electronic devices, including mobile devices and portable computers using all forms of radio networks. Examples of such radio networks may include Bluetooth™ based radio systems and IEEE 802.11b standard based radio systems designed for connecting a variety of mobile devices in a secure ad-hoc fashion. However, for the sake of simplicity, discussions will concentrate mainly on an example Bluetooth™ based radio system for providing ad-hoc security services of varying complexity for electronic devices equipped with Bluetooth technology, although the scope of the present invention is not limited thereto.

As set forth in the "*Specification of the Bluetooth System*" by the Bluetooth Special Interest Group (SIG) at http://www.bluetooth.com/, Bluetooth™ wireless technology is a low-cost, low-power, short-range radio link for mobile devices and for WAN/LAN access points to offer fast and reliable digital transmissions of both voice and data over the globally available 2.4 GHz ISM (Industrial, Scientific and Medical) band without the need for a central network. Current Bluetooth™ based systems may provide up to 100-meter range capability (but extendable to more than 100 meters) and an asymmetric data transfer rate of 721 kb/sec between

mobile devices and fixed voice/data access points (known as Bluetooth Access Points "BTAPs").

The Bluetooth™ protocol supports a maximum of three voice channels for synchronous, CVSD-encoded transmission at 64 kb/sec, and treats all radios as peer units identified by unique 48-bit addresses in compliance with the Bluetooth specification. At the start of any connection, the initiating device is a temporary master. This temporary assignment, however, may change after initial communications are established. Each master device may have active connections of up to seven slave devices. Such a connection between a master device and one or more slave devices forms a "piconet." Link management allows communication between piconets, thereby forming "scattemets." Typical Bluetooth™ master devices include cordless phone base stations, local area network (LAN) access points, laptop computers, or bridges to other networks. Bluetooth™ slave devices may include cordless handsets, cell phones, headsets, personal digital assistants, digital cameras, or computer peripherals such as printers, scanners, fax machines and other electronic devices.

Bluetooth™ protocol also utilizes time-division duplex (TDD) to support bi-directional communications between mobile devices and BTAPs. Frequency hopping spread-spectrum technology accommodating frequency diversity permits operation in noisy environments and permits multiple piconets to exist in close proximity. This is so since frequency diversity is inherent in frequency hopping, especially when it is wide, as in the case of Bluetooth™ (spread over a band of about 80 MHz). The frequency hopping transmission hops at a rate of 1600 hops per second over 791-MHz channels between 2402 MHz and 2480 MHz. Various error-correcting schemes permit data packet protection by 1/3- and 2/3-rate forward error correction.

Attention now is directed to the drawings and particularly to FIG. 1, an example Bluetooth™ based security system according to an embodiment of the present invention is illustrated. Such a Bluetooth™ based security system may be installed in a designated area such as a company site, a school, a building or an industry complex to provide ad-hoc security services for electronic devices such as portable computers equipped with Bluetooth (BT) without the need for cables, chains or other mechanical components. The Bluetooth™ based security system serves to control and monitor the status of all secured devices or assets remotely, through the Internet or other networks whenever possible.

As shown in FIG. 1, the Bluetooth™ based security system 100 comprises a central security server (SS) (also known as "security provider") 110, a network of Bluetooth (voice/data) Access Points (BTAPs) 120A-120N and one or more secured devices (SD) 130 equipped with Bluetooth™ technology. All BTAPs 120A-120B may be strategically located at designated points where users are most likely to secure BT equipped devices temporarily (or permanently). The BTAPs 120A-120N may server to connect a secured device (SD) 130 to a communicating device via a secure (private) wireless link. For example, a secured device (SD) 130 such as a portable computer equipped with Bluetooth™ technology may link to a mobile phone (for example) that uses Bluetooth™ technology to connect to the Internet to access e-mail. Each BTAP 120A-120N may be installed at a pre-surveyed (known) location to establish a BT link for communication with the secured device (SD) 130 and enabling the secured device (SD) 130 to access the security server (SS) 110 and the Internet, for example.

The central security server 110 may be connected directly or indirectly to all the BTAPs

120A-120N in the network, and may serve as a central point relative to the physical structure that houses the network of BTAPs 120A-120N. The central security server 110 may be connected to the Internet or other networks to provide security services, including remote monitoring and tracking of the secured device (SD) 130.

FIG. 2 illustrates an example system platform of a security server (SS) 110 according an embodiment of the present invention. As shown in FIG. 2, the secured server (SS) 110 may include, but not limited to, a processor subsystem 210, a data storage subsystem 220, and an I/O subsystem including an input device 240 and an output device 250.

The processor subsystem 210 may include one or more processors or central processing units (CPUs) such as Intel® i386, i486, Celeron™ or Pentium® processors. The data storage subsystem 220 may include a volatile memory (e.g., random-access-memory "RAM") for database 220A and a non-volatile memory (e.g., read-only-memory "ROM") for containing a security control software 220B to provide ad-hoc security services, including remote monitoring and tracking of secured assets (i.e., secured device 130) of the Bluetooth™ based security system 100, including searching and capturing the location of the lost or stolen secured device (SD) 130. The input device 240 may include a keyboard controller for controlling operations of an alphanumeric keyboard, a cursor control device such as a mouse, track ball, touch pad, joystick, and bar code reader for enabling an IT administrator (for example) to install the security control software 220B and change system settings and configurations. The output device 250 may include a printer, a display monitor, speakers and network devices for establishing connections with the Internet or other networks to provide security services, including remote monitoring and

tracking of the secured device (SD) 130.

FIG. 3 illustrates an example system platform of a secured device (SD) 130 such as a portable computer according an embodiment of the present invention. As shown in FIG. 3, the secured device (SD) 130 may include, but not limited to, a processor subsystem 310, a host chipset 320, a memory 330 connected to the host chipset 320, a graphics/display subsystem 340 connected to the host chipset 320, the I/O subsystem 350 connected to the host chipset 320, a Bluetooth transceiver 360 including an antenna complex 362 arranged to establish communication with any of the BTAPs 120A-120N for security services and optionally, a Global Positioning System (GPS) receiver 370 including an antenna complex 372 or other satellite or land-based network arranged to provide radio positioning and navigation needs, including receiving information relating to the location or position of the secured device (SD) 130 relative to the BTAPs 120A-120N and determining a change in distance between the secured device (SD) 130 and a particular BTAP (e.g., ranging measurement from the BTAP).

The processor subsystem 310 may also include one or more processors or central processing units (CPUs) such as Intel® i386, i486, Celeron™ or Pentium® processors.

The memory 330 may correspond to a dynamic random-access-memory (DRAM), but may be substituted for read-only-memory (ROM), video random-access-memory (VRAM) and the like. Such a memory 330 may store an operating system (OS) 330A such as Windows™ 95/98 and Windows™ 2000 for use by the processor subsystem 310, and information and instructions such as a security control software 330B for activating/deactivating a lock with the BTAPs 120A-120N of the Bluetooth™ based security system 100.

The graphics/display subsystem 240 may include, for example, a graphics controller, a local memory and a display monitor (e.g., cathode ray tube, liquid crystal display, flat panel display, etc.).

The IO subsystem 250 may provide an interface with a variety of I/O devices and the like, such as: a Peripheral Component Interconnect (PCI) bus (PCI Local Bus Specification Revision 2.2 as set forth by the PCI Special Interest Group (SIG) on December 18, 1998) which may have one or more I/O devices connected to PCI slots, an Industry Standard Architecture (ISA) or Extended Industry Standard Architecture (EISA) bus option, and a local area network (LAN) option for communication peripherals such as telephone/fax/modem adapters, answering machines, scanners, personal digital assistants (PDAs) etc; a super I/O chip (not shown) for providing an interface with another group of I/O devices such as a mouse, keyboard and other peripheral devices; an audio coder/decoder (Codec) and modem Codec; a plurality of Universal Serial Bus (USB) ports (USB Specification, Revision 2.0 as set forth by the USB Special Interest Group (SIG) on April 27, 2000); and a plurality of Ultra/66 AT Attachment (ATA) 2 ports (X3T9.2 948D specification; commonly also known as Integrated Drive Electronics (IDE) ports) for receiving one or more magnetic hard disk drives or other I/O devices.

The USB ports and IDE ports may be used to provide an interface to a hard disk drive (HDD) and compact disk read-only-memory (CD-ROM). I/O devices may include, for example, a keyboard controller for controlling operations of an alphanumeric keyboard, a cursor control device such as a mouse, track ball, touch pad, joystick, etc., a mass storage device such as magnetic tapes, hard disk drives (HDD), and floppy disk drives (FDD), and serial and parallel

ports to printers, scanners, and display devices.

The host chipset 220 may correspond to, for example, in Intel® 810, Intel® 870 and 8XX series chipsets which include, for example, a memory controller hub (MCH) for controlling operations of the main memory 330 and an IO controller hub (ICH) for controlling operations of a variety of I/O devices, via standard PCI, ISA or EISA bus.

The Bluetooth transceiver 360 contains an identification (ID) number unique to the secured device (SD) 130 for identification and lock-in communication with any one of the BTAPs 120A-120N strategically located at designated points where the secured device (SD) 130 is most likely secured temporarily (or permanently). Such a Bluetooth transceiver 360 typically provides compatibility between the radio waves used in the Bluetooth™ based security system 100. As shown in FIG. 4, the Bluetooth transceiver 360 typically includes a radio-frequency (RF) unit 410 arranged to transmit/receive radio waves to/from any one of the BTAPs 120A-120N, via the antenna complex 362; a baseband unit 420 arranged to establish link set-up (control) and support for link management between the secured device (SD) 130 and the BTAPs 120A-120N in compliance with the "*Specification of the Bluetooth System*", including user authentication and link authorization; and optionally, a Bluetooth data processor 430 arranged to process sample Bluetooth data, including the location of the last BTAP that the secured device (SD) 130 connected thereto.

In one example embodiment, the Bluetooth transceiver 360 can determine information relating to the location or position of the secured device (SD) 130 relative to the BTAPs 120A-120N by communicating with several BTAPs 120A-120N.

The GPS receiver (sensor) 370 may be part of an accurate three-dimensional global positioning satellite (GPS) system to provide radio positioning and navigation needs. As shown in FIG. 5, the GPS receiver 370 may also include a radio-frequency (RF) unit 510 arranged to receive GPS data from a plurality of GPS satellites (not shown), via the antenna complex 372; a baseband unit 520 arranged to sample GPS data; and optionally, a GPS data processor 530 arranged to process sample GPS data relating to the location or position of the secured device (SD) 130 relative to the BTAPs 120A-120N and determine a change in distance between the secured device (SD) 130 and a particular BTAP (e.g., ranging measurement from the BTAP).

More specifically, the GPS receiver 370 may track pseudo-random noise from a plurality of GPS satellites, via the antenna complex 372 and generate therefrom time-of-arrival values. Thereafter, the GPS data processor 530 may sample the time-of-arrival values from the GPS constellation for each of the GPS satellites (not shown) and multiply the sample data by the speed of light to produce a plurality of pseudo-range measurements. The GPS data processor 530 then adjusts these pseudo-range measurements to compensate for deterministic errors such as the difference between each satellite's clock and GPS system time, atmospheric distortion of GPS signals and other considerations such as relativity factors. The GPS data processor 530 may include an instruction set which gathers the information necessary to compute adjustments to the pseudo-range measurements from a 50 Hz digital data stream which the GPS satellites broadcast along with their precision and coarse acquisition code. After the GPS data processor 530 makes all the necessary adjustments to the pseudo-range measurements, the position/time solution process may then be performed to determine the present GPS receiver antenna position.

The GPS data processor 530 may compute its X, Y, Z position fix in terms of the World Geodetic System adapted in 1984, which is the basis on which the GPS develops its worldwide common grid references. Generally, the X, Y, Z coordinates are converted to latitude, longitude and altitude map datum prior to output. The GPS position solution is intrinsically referenced to the electrical phase center of the antenna. Finally, the GPS data processor 520 may compute clock bias results which are one of the parameters to be considered in addition to the X, Y, Z coordinates. The clock bias may be computed in terms of the time offset of the clock in the GPS receiver 370 versus GPS system time. Accordingly, the secured device (SD) 130 receives the GPS position data which information is processed to establish the present position of the secured device (SD) 130 relative to the BTAPs 120A-120N.

Both the Bluetooth transceiver 360 and the GPS receiver 370 may be integrated into the host chipset 220 as system-on-chip designs that is compatible with ASIC (Application-Specific Integrated Circuit) design flows. Alternatively, the Bluetooth subsystem 260 and the GPS subsystem 270 may be separate "plug-and-play" modules or a single "plug-and-play" module, including the ASIC and passive components for communications over longer distances.

FIG. 6 illustrates an example Bluetooth and GPS subsystem 360 and 370 of the secured device (SD) 130 according to an embodiment of the present invention. As shown in FIG. 6, the Bluetooth and GPS subsystem may include, but not limited to, a Bluetooth/GPS radio-frequency (RF) unit 610, a radio interface 620, a GPS tracking unit 630, and a Bluetooth/GPS data processor 640. The Bluetooth/GPS radio-frequency (RF) unit 610 may track both GPS data (pseudo-random noise form a plurality of GPS satellites) and Bluetooth data, via an integrated

antenna complex (not shown) under control of the GPS tracking unit 630. The Bluetooth/GPS data processor 640 may then process GPS data and Bluetooth data substantially the same way as described with reference to FIGs. 4 and 5.

Referring back to FIG. 1, the operation of the central security server (SS) 110, the BTAP 120A, for example, and the secured device (SD) 130 of the Bluetooth™ based security system 100 may be described as follows:

When a secured device (SD) 130 equipped with Bluetooth™ (also known as "client device") makes a BT connection with any of the BTAPs 120A-120N capable of providing security, two important attributes of the secured device (SD) 130 are captured by the BTAP 120A-120N and registered in the database 220A maintained at the central security server (SS) 110 (see FIG. 2). These attributes includes (1) the unique device ID of the secured device (SD) 130, and (2) the last known location of the secured device (SD). The attributes may be derived from the location of the last BTAP 120A-120N that the secured device (SD) 130 connected thereto, or alternatively, may be obtained through an onboard GPS receiver 370.

The BTAP 120A, for example, may in turn provide its own (known) location (X, Y, Z coordinates) to the secured device (SD) 130. The secured device (SD) 130 may choose to use this information (X, Y, Z coordinates) in a variety of different ways. One of the ways, as mentioned above, is to provide this information to facilitate its next connection with another one of the BTAPs 120A-120N.

The central security server (SS) 110 may be configured, via the security control software 220B, to log the information provided by the BTAPs 120A-120N, to activate and maintain lock

with the secured device (SD) 130, and provide an "unlock code" (which may be randomly selected) to the secured device (SD) 130 upon request from the secured device (SD) 130 for storage for future use, and subsequently notify the owner (user) of the secured device (SD) 130 if the secured device (SD) 130 is lost or stolen due to a BT disconnection.

The lock mechanism (i.e., security control software 220B and 330B shown in FIGs. 2-3) between the central security server (SS) 110, the BTAPs 120A-120N and the secured device (SD) 130 may be activated in two ways: (1) when the secured device (SD) 130 proactively requests that it be locked with the current BTAP 120A, as shown in FIG. 1; and (2) when the central security server (SS) 110 uses a pre-defined timeout value to engage the lock between the secured device (SD) 130 and the current BTAP 120A after the secured device (SD) 130 has established a BT connection with the current BTAP 120A. Typically the secured device (SD) 130 may be locked to the current BTAP 120A after the secured device (SD) 130 has established a BT connection with the current BTAP 120A for several minutes or more.

The lock mechanism consists of logging and maintaining the secured device (SD) 130 attributes specified above in a suitable database 220A at the central security server (SS) 110 (see FIG. 2 for example). After the central server (SS) 110 logs the secured device (SD) 130 attributes in its database 220A, an "unlock code" may be provided to the secured device (SD) 130 for storage for future use.

For a small fee (or no fee) the owner of the locked device (SD) 130 may remotely query the status of the secured asset(s). In addition, the central security server (SS) 110 can notify the owner (or security personnel) if any secured device (SD) 130 is "lost" through unauthorized

disconnection.

After the secured device (SD) 130 has received the unlock code, the power supply to all internal components may be shut down, except those required to maintain the BT connection with the BTAPs 120A-120N.

The owner of the secured device (SD) 130 may disengage the lock by triggering it to send the unlock code to the central security server (SS) 110. The central security server (SS) then checks to make sure that the secured device (SD) 130 being unlocked is not in a search and arrest mode and removes the entry for the specified device, making the secured device (SD) 130 free to roam.

In the event of a theft, the security server (SS) 110 will note the broken BT link with the secured device (SD) 130, and notify appropriate personnel along with the last known position of the secured device (SD) 130. Additionally the security server (SS) 110 can initiate a network wide (or Internet wide) search and arrest request for the specified device ID and unlock code. If an attempt is made to use the stolen device 130, the stolen device 130 will first attempt to re-establish the BT connection that existed before it was stolen, using the stored unlock code. Until such a connection can be established, and the secured device (SD) 130 systematically unlocked, the secured device (SD) 130, if lost of stolen, will remain inoperable and serve as a theft deterrent.

Turning now to FIG. 7, an example lock activation procedure between a security server (SS) 110 and a secured device (SD) 130 of the Bluetooth™ based security system 100 according to an embodiment of the present invention is illustrated. As shown in FIG. 7, the Bluetooth™

based security system 100 activates the lock between the security server (SS) 110 and the secured device (SD) 130, via the BTAP 120A, at block 710, in two ways: (1) when the secured device (SD) 130 proactively requests to activate lock with the current BTAP 120A, or (2) when a pre-defined timeout value of the security server (SS) 110 is expired after the secured device (SD) 130 has established a BT connection with the current BTAP 120A.

Next, the security server (SS) 110 connected to the current BTAP 120A and the secured device (SD) 130 may proceed to exchange parameters for locking at block 720. At this time, the security server (SS) 110 transmits two items to the secured device (SD) 130, via the current BTAP 120A through the BT link, including the location information (X, Y, Z coordinates) of the current BTAP 120A and the unlock code to the secured device (SD) 130 for future use. In return, the secured device (SD) 130 transmits two items back to the security server (SS) 110, via the current BTAP 120A through the BT link, including the unique device ID of the secured device (SD) 130 and the last know location (X, Y, Z coordinates) of the secured device (SD) 130.

Afterwards, the secured device (SD) 130 may power down all internal components except those required to maintain the BT connection with the security server (SS) 110, via the current BTAP 120A at block 730. The lock between the security server (SS) 110 and the secured device (SD) 130 may then be maintained at block 740.

FIG. 8 illustrates an example parameter exchange procedure for locking between the security server (SS) 110 and a secured device (SD) 130 of the Bluetooth™ based security system 100 in more detail. During block 720 shown in FIG. 7, the security server (SS) 110 transmits

two items to the secured device (SD) 130, via the current BTAP 120A through the BT link, including the location information (X, Y, Z coordinates) of the current BTAP 120A and the unlock code to the secured device (SD) 130 at block 810. The secured device (SD) 130 then transmits two items back to the security server (SS) 110, via the current BTAP 120A through the BT link, including the unique device ID of the secured device (SD) 130 and the last know location (X, Y, Z coordinates) of the secured device (SD) 130 at block 820. The security server (SS) 110 then creates log entry in its database 220A, stores the unique device ID of the secured device (SD) 130, the last known location (X, Y, Z coordinates) of the secured device (SD) 130, the time, and the unlock code etc., at block 830. The secured device (SD) 130 then stores the unlock code transmitted from the security server (SS) 110 at block 840 for future use. Afterwards, the secured device (SD) 130 powers down all internal components except those required to maintain the BT connection with the security server (SS) 110, via the current BTAP 120A at block 730.

FIG. 9 illustrates an example lock maintenance procedure of the Bluetooth™ based security system 100 according to an embodiment of the present invention. At block 910, if there is an occurrence of an unauthorized breach event during the time when the lock between the security server (SS) 110 and the secured device (SD) 130 is maintained at block 740, the security server (SS) 110 may assume that the secured device (SD) 130 is lost or stolen, and operate in a search and arrest mode to notify an appropriate personnel along with the last known position of the secured device (SD) 130 at block 920. An unauthorized breach event is triggered if there is an unauthorized BT disconnection with the secured device (SD) 130. The security server (SS)

110 can initiate a network wide (or Internet wide) search and arrest request for the specified device ID and unlock code. If an attempt is made to use the stolen device 130, the stolen device 130 will first attempt to re-establish the BT connection that existed before it was stolen, using the stored unlock code. Until such a connection can be established, and the secured device (SD) 130 systematically unlocked, the stolen device 130 will remain inoperable.

FIG. 10 illustrates an example search and arrest procedure of the Bluetooth™ based security system according to an embodiment of the present invention. When the security server (SS) 110 is in a search and arrest mode at block 920, the security server (SS) 110 updates the log to indicate that the secured device (SD) 130 is lost or stolen at block 1010. Optionally, for a small fee (or no fee) the owner of the locked device (SD) 130 may remotely query the status of the secured device (SD) 130. In addition, the central security server (SS) 110 can notify the owner (or security personnel) if the secured device (SD) 130 is "lost" or "stolen" through unauthorized disconnection, and launch the network wide search and arrest request, via the Internet or other networks to locate the stolen device 130 at block 1020.

If the stolen device 130 ever tries to access the Internet or other networks at block 1030, the security server (SS) 110 may capture the location of the stolen device 130 and notify the recovery team of the location of the stolen device 130 at block 1040 in order to recover the stolen device 130 at block 1050.

FIG. 11 illustrates an example lock deactivation procedure of the Bluetooth™ based security system according to an embodiment of the present invention. If the user (owner) of the secured device (SD) 130 desires to disengage the lock and move the secured device (SD) 130 to

a different location in the Bluetooth™ based security system, the lock must first be deactivated by the user (owner) with the proper "unlock code". Otherwise, an unauthorized breach event may be triggered, and the security server (SS) 110 may initiate a network wide (or Internet wide) search and arrest request for the secured device (SD) 130.

As shown in FIG. 11, the deactivation of lock may be triggered at the security server (SS) 110 when the secured device (SD) 130 is about to experience a broken BT link with the security server (SS) 110 at block 1110. The security server (SS) 110 may prompt the user at the secured device (SD) 130 to input the unlock code at block 1120. Next, the security server (SS) 110 may verify the user supplied unlock code with the unlock code stored at block 1130. The security server (SS) 110 then determines if the user supplied unlock code matches the stored unlock code at block 1140. If the user supplied unlock code matches the stored unlock code, then the security server (SS) 110 may unlock or disengage the lock with the secured device (SD) 130 at block 1150. At this time, the security server (SS) 110 may check if the secured device (SD) 130 being unlocked is not part of the search and arrest request and then remove the entry for the specified device, making the secured device (SD) 130 free to roam.

However, if the user supplied unlock code does not match the stored unlock code, the security server (SS) 110 may allow the user to re-enter the unlock code two or three times, for example, before making the decision that the user of the secured device (SD) 110 is not the rightful owner of the secured device (SD) 130. As a result, an unauthorized breach event may be triggered. the security server (SS) 110 may then initiate a network wide (or Internet wide) search and arrest request for the secured device (SD) 130.

For Bluetooth equipped devices, there is no need to use additional hardware and communications specifically for identification and tracking applications. As described in this invention, the Bluetooth network can be setup to provide access control, tracking and security services of varying complexity without any additional hardware overheads. A security control software system 220B and 330B shown in FIGs. 2-3 may be deployed by an IT administrator to track IT funded notebooks, for example, through site wide Bluetooth Access Points (BTAPs). Such a software system may be a software module provided on a tangible medium, such as a floppy disk or compact disk (CD) ROM, or via Internet downloads, which may be available for an IT administrator to conveniently plug-in or download into the host operating system (OS). Such software modules may also be available as a firmware module or a comprehensive hardware/software module which may be built-in the host. In addition, method steps of FIGs. 7-11 may be performed by a computer processor executing instructions organized into a program module or a custom designed state machine. Storage devices suitable for tangibly embodying computer program instructions include all forms of non-volatile memory including, but not limited to: semiconductor memory devices such as EPROM, EEPROM, and flash devices; magnetic disks (fixed, floppy, and removable); other magnetic media such as tape; and optical media such as CD-ROM disks.

While there have been illustrated and described what are considered to be exemplary embodiments of the present invention, it will be understood by those skilled in the art and as technology develops that various changes and modifications may be made, and equivalents may be substituted for elements thereof without departing from the true scope of the present

invention. For example, the Bluetooth based security system as shown in FIG. 1 may be configured differently or employ some or different components than those illustrated. As an alternative short-range wireless communication embodiment, IEEE 802.11b standards systems may be utilized as a wireless local area network (LAN) developed by the Institute of Electrical and Electronic Engineering (IEEE) Institute in order to specify an "over the air" interface between a wireless client and a base station or access point (AP), as well as among wireless clients. Transceivers may use the IEEE 802.11b standard to communicate with transmitters using the IEEE 802.11b standard and with each other to determine position relative to the transmitters. In addition, the security server (SS) 110 and the secured device (SD) 130 as shown in FIGs. 2-3 may be configured differently or employ some or different components than those illustrated without changing the basic function of the invention. Likewise, the Bluetooth transceiver 360 and the GPS receiver 370 as shown in FIGs. 4-6 may also be configured different without changing the basic function of the invention. Further, the software program installed at the security server (SS) 110 and the secured device (SD) 130 may be designed to perform the same task as shown in FIGs. 7-11. Many modifications may be made to adapt the teachings of the present invention to a particular situation without departing from the scope thereof. Therefore, it is intended that the present invention not be limited to the various exemplary embodiments disclosed, but that the present invention includes all embodiments falling within the scope of the appended claims.

What is claimed is: